Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Gouvernement du Canada Livre blanc : Souveraineté des données et nuage public

Publié : le 2018-06-25

© Sa Majesté la Reine du chef du Canada,
représentée par le président du Conseil du Trésor, 2018

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

N° de catalogue BT22-213/2018F-PDF
ISBN: 978-0-660-27234-4

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Government of Canada White Paper: Data Sovereignty and Public Cloud

Gouvernement du Canada | Government of Canada

Gouvernement du Canada Livre blanc : Souveraineté des données et nuage public

Du Secrétariat du Conseil du Trésor du Canada

Le gouvernement du Canada (GC) a une stratégie « Le nuage d'abord » selon laquelle les services d'informatique en nuage sont considérés et évalués comme principale option de prestation lorsqu'il entreprend des investissements, des initiatives, des stratégies et des projets de technologie de l'information (TI). Les ministères et les organismes doivent examiner les modèles de déploiement des services d'informatique en nuage dans l'ordre de priorités qui suit :

1. nuage public;
2. nuage hybride;
3. nuage privé;
4. hors-nuage.

La stratégie « Le nuage d'abord » se reflète dans les récentes mises à jour de la Politique sur la gestion de la technologie de l'information du Conseil du Trésor (section 6.2.6).

Le Secrétariat du Conseil du Trésor du Canada (SCT), en consultation avec les ministères clés [1], a déterminé que dans certaines conditions, un nuage public commercial peut offrir une protection suffisante pour les données allant jusqu'au niveau Protégé B. À ce titre, l'approvisionnement par « nuage protégé » sera lancé en 2018 afin de rendre les services d'informatique en nuage publics commerciaux accessibles aux ministères pour le stockage de données allant jusqu'au niveau Protégé B.

Sur cette page

- Objet du présent document
- Éléments hors de la portée de ce document
- En quoi consiste l'informatique en nuage?

- Défis liés au nuage public
- Relever les défis
- Souveraineté des données : Risques et mesures d'atténuation
- Équilibrer les risques en matière de sécurité et les avantages commerciaux
- Sommaire
- Prochaines étapes
- Annexe A : Réponses du gouvernement concernant la souveraineté des données

Objet du présent document

Le présent document vise à donner un aperçu du risque pour la souveraineté des données [2] ainsi que du risque pour la résidence des données [3] et la sécurité des données, qui ont trait à l'utilisation de services d'informatique en nuage publics commerciaux. On examine ces risques dans le contexte de la stratégie « Le nuage d'abord » du gouvernement du Canada (GC). À la fin du document, le lecteur comprendra les risques et les mesures d'atténuation qui s'appliquent. En effet, il aura aussi appris en quoi les services d'informatique en nuage peuvent aider le GC à gérer d'autres risques, notamment :

- vieillissement de la TI;
- lacunes actuelles en matière de sécurité;
- manquement à bénéficier des technologies émergentes.

Éléments hors de la portée de ce document

Le présent document ne constitue ni une vue d'ensemble exhaustive des services d'informatique en nuage publics ni une orientation stratégique du GC au regard de ces services. D'autres documents comme le Plan stratégique du gouvernement du Canada pour la gestion de l'information et la technologie de l'information de 2017 à 2021 et la Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada sont disponibles et fournissent des renseignements sur les services d'informatique en nuage et l'orientation stratégique.

En quoi consiste l'informatique en nuage?

L'informatique en nuage est la prestation de ressources informatiques sur demande (allant des applications aux centres de données) par Internet, moyennant un coût pour chaque consultation. Les services d'informatique en nuage peuvent être déployés selon trois modèles différents : public, privé et hybride.

Dans le modèle de nuage public, les ressources d'informatique en nuage (c.-à-d. le matériel, les logiciels et l'infrastructure) appartiennent à un fournisseur de services d'informatique en nuage (FSIN). Les organisations accèdent aux services de la TI par Internet à partir d'un bassin de ressources partagées qui sont séparées les unes des autres de façon logique. Selon le modèle de l'informatique en nuage privé, les ressources informatiques (qui peuvent se trouver sur place ou être hébergées par un FSIN tiers) sont réservées à une seule organisation, et elles sont gérées dans un réseau privé. Selon le modèle du nuage hybride, une infrastructure combinée des secteurs public et privé est utilisée, les données et les applications communiquant entre les deux.

Défis liés au nuage public

Titres de la section

- Sécurité des données
- Résidence des données
- Souveraineté des données

L'informatique en nuage introduit un important changement dans la façon dont les services de la TI sont livrés, et le GC doit se positionner pour tirer profit de ce nouveau modèle de prestation de services. Par contre, étant donné que la nature de l'informatique en nuage entraîne pour une organisation le changement de la portée du contrôle de ses ressources d'information, on a soulevé les défis dans le contrôle, la protection et la confidentialité des données au GC :

- sécurité des données;
- résidence des données;
- souveraineté des données.

Sécurité des données

Lorsque les données sont transférées dans le nuage, la sécurité devient une responsabilité partagée avec les FSIN. Les FSIN sont responsables de la sécurité **du** nuage, et les ministères du GC sont responsables de la sécurité **à destination, en provenance et dans** le nuage. Une simple analogie serait un immeuble loué. Les propriétaires ou les gérants d'immeubles sont responsables de la sécurité de l'immeuble et des aires communes, mais les locataires sont responsables des mesures de sécurité dans les unités qu'ils louent. Ce modèle modifié de la portée du contrôle et de la responsabilité partagée suscite souvent des craintes que la position de sécurité d'une organisation soit dégradée.

Étude de cas : Royaume-Uni et approche axée sur la gestion des risques

En 2013, le gouvernement du Royaume-Uni a introduit une politique « Cloud First » (le nuage d'abord) et un virage vers une approche au regard de la gestion des risques pour l'utilisation des services d'informatique en nuage. La stratégie de l'informatique en nuage du Royaume-Uni (en anglais seulement) n'impose aucune limite géographique sur les services d'informatique en nuage publics en ce qui concerne les renseignements classés comme officiels (il y a des limites pour les renseignements classés comme secret et très secret). Le National Cyber Security Centre du Royaume-Uni a plutôt adopté et appuyé une approche axée sur la gestion des risques, suivant les 14 principes de sécurité de l'informatique en nuage (en anglais seulement) que doivent examiner les organisations au moment d'évaluer un service d'informatique en nuage. Le principe de sécurité de l'informatique en nuage nº 2, protection et résilience des actifs, souligne la nécessité pour les organisations du secteur public de comprendre :

- dans quels pays les données seront stockées, traitées et gérées, et comment ces pays influenceront la conformité avec les lois pertinentes;
- si le territoire de compétence juridique dans laquelle le fournisseur de services exerce ses fonctions est acceptable pour l'organisation.

Résidence des données

En général, les FSIN sont des fournisseurs à grande échelle, ce qui signifie que leurs services sont déployés partout au monde, outrepassant les actifs de la TI du GC. Bien que les FSIN aient la capacité de déplacer les données d'un consommateur n'importe où dans le monde, le consommateur peut isoler ses données dans une région géographique donnée. Il s'agit d'une caractéristique importante pour les consommateurs, car elle leur permet de protéger leurs données en vertu des lois et des politiques d'un territoire donné. Le déplacement des données du GC à l'extérieur des frontières géographiques du Canada peut avoir une incidence sur sa capacité d'accéder aux données et aux services, qui sont essentiels à la poursuite des activités du GC.

Souveraineté des données

Peu importe l'emplacement géographique des ressources d'informatique en nuage, les données hébergées dans le nuage peuvent être assujetties aux lois d'autres pays. Comme il a déjà été mentionné, les FSIN sont des fournisseurs à grande échelle, affichant un déploiement mondial. Par conséquent, un FSIN qui mène des activités à l'étranger pourrait être tenu de

respecter un mandat, une ordonnance d'un tribunal ou une demande d'assignation d'un organisme d'application de la loi étranger qui cherche à obtenir des données du GC. Cela signifie que le Canada, lorsqu'il stocke des données dans le nuage, ne peut pas assurer la pleine souveraineté de ses données. Le manque de pleine souveraineté des données risque de nuire au GC et à ses tierces parties. Les données sensibles du GC pourraient être assujetties à des lois étrangères et divulguées à un autre gouvernement. En vertu de certaines lois étrangères, les données du GC pourraient être divulguées sans préavis au GC.

Étude de cas : Colombie-Britannique et résidence des données intégrale

Le Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique a publié des lignes directrices sur l'informatique en nuage pour les organismes publics (PDF (Portable Document Format), 175 KO (Kilo octets)) (en anglais seulement) (mises à jour en juin 2012) afin de fournir des conseils au sujet de l'application de la Loi sur l'accès à l'information et la protection de la vie privée (FIPPA) de la Colombie-Britannique. La FIPPA s'applique aux **renseignements personnels** qui sont **sous la garde ou le contrôle d'un organisme public**. Des mesures rigoureuses visant la résidence des données ont été mises en place afin de veiller à la protection des renseignements personnels et au respect de la FIPPA. Aux termes des lignes directrices et sous réserve de quelques exceptions, les organismes publics de la Colombie-Britannique doivent :

- veiller à ce que les renseignements personnels soient stockés et accessibles à partir du Canada seulement;
- protéger les renseignements personnels en prenant des mesures de sécurité raisonnables contre les risques d'accès, de collecte, d'utilisation, de divulgation et d'élimination non autorisés.

Relever les défis

▾ Titres de la section

- Sécurité des données
- Résidence des données
- Souveraineté des données

Le GC a réalisé des progrès dans ses efforts pour relever les défis liés à la sécurité des données, à la résidence des données et à la souveraineté des données afin de permettre l'adoption de l'informatique en nuage.

Sécurité des données

Comme il a déjà été mentionné, étant donné la responsabilité partagée en matière de sécurité dans le nuage et la couverture à grande échelle des FSIN, le GC doit utiliser différents processus, lorsqu'il utilise le nuage, afin de répondre aux exigences des politiques en matière de gestion des risques pour la sécurité. Les FSIN ne s'évaluent pas en fonction des lignes directrices du GC comme les ITSG-33 [4], mais ils ont obtenu les certifications reconnues à l'échelle internationale comme ISO 27001. Le GC a publié le Profil de contrôle de sécurité pour les services de la TI du GC fondés sur l'informatique en nuage qui renvoie à ITSG-33 par les certifications communes dans l'industrie de l'informatique en nuage. Le GC a aussi publié l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) pour aider les ministères et les organismes à comprendre les exigences actuelles de la politique sur la sécurité du SCT dans le contexte de l'informatique en nuage. L'AMOPS met en lumière les mesures suivantes :

- principales mesures de sécurité nécessaires pour protéger l'information et les actifs du GC dans un environnement de l'informatique en nuage;
- mesures de contrôle de la sécurité qui relèvent du FSIN et du ministère.

Résidence des données

Le GC a publié l'Orientation relative à la résidence des données électroniques (AMPTI), qui établit les exigences canadiennes en matière de résidence des données classées dans les catégories Protégé B, Protégé C ou Classifiées. Ces exigences sont intégrées dans les récentes mises à jour de la Politique sur la gestion de la technologie de l'information du Conseil du Trésor (section 6.2.7). Cependant, le fait de limiter la résidence des données au Canada entraîne deux nouveaux risques :

1. Limiter la disponibilité des solutions sur le marché. Au moment de la rédaction du présent document, au moins cinq des plus grands FSIN avaient la capacité d'isoler les données au Canada.
2. Créer un obstacle au commerce. Les considérations commerciales et le risque juridique connexe font l'objet de conseils juridiques formulés par le ministère de la Justice Canada dans le contexte des récentes mises à jour apportées à la Politique sur la gestion de la technologie de l'information. Lorsqu'il s'agit d'obtenir des services d'informatique en nuage, les ministères voudront peut-être examiner ces conseils.

Souveraineté des données

En autant qu'un FSIN menant ses activités au Canada soit assujetti aux lois d'un pays étranger, le Canada n'aura pas la pleine souveraineté sur ses données, car il y a toujours le risque qu'un autre pays accède aux données stockées dans le nuage. La question de la souveraineté des données est complexe, et elle évolue continuellement au fur et à mesure que les lois étrangères sont mises à l'essai dans les tribunaux étrangers.

Souveraineté des données : Risques et mesures d'atténuation

Titres de la section

- Limiter les catégories de données stockées dans le nuage
- Chiffrement des données
- Clauses contractuelles types pour le nuage

Dans l'environnement de nuage public, les données du gouvernement sont confiées à une tierce partie qui peut être assujettie aux lois d'un pays étranger, même si les données résident au Canada. De ce fait, le principal risque pour le GC en ce qui concerne la souveraineté des données est que les organismes étrangers peuvent tirer parti des lois de leur pays d'origine pour obliger les FSIN à transmettre les données du GC, ce qui pourrait :

- causer des dommages au GC;
- entraîner les Canadiens à perdre confiance en leur gouvernement.

Il convient de souligner que de nombreux pays, y compris le Canada, ont des lois qui leur permettent d'assigner à témoigner ou d'obtenir un mandat pour obtenir des renseignements d'organisations privées en guise d'appui d'enquêtes juridiques. Les principaux risques pour la souveraineté des données sont la Foreign Intelligence Surveillance Act (FISA) des États-Unis et la capacité du gouvernement américain d'obliger une organisation assujettie à la loi américaine à transmettre des données sous son contrôle, peu importe son emplacement, et sans en informer le Canada. Il est important de mentionner qu'il existe depuis longtemps des accords d'échange de renseignements entre les organismes de sécurité et d'application de la loi du Canada et des États-Unis. Ces ententes de longue date ainsi que des traités d'entraide juridique sont d'autres moyens par lesquels les États-Unis peuvent accéder aux renseignements hébergés au Canada.

Le GC recommande un certain nombre de mesures d'atténuation pour réduire le risque d'accès non autorisé à des renseignements de nature délicate, notamment :

- limiter les catégories de données stockées dans le nuage;

- chiffrer les données;
- utiliser des clauses contractuelles types.

Limiter les catégories de données stockées dans le nuage

Suivant l'exemple d'autres pays, le Canada limitera les catégories de données qui peuvent être stockées dans le nuage. Jusqu'à ce jour, les principaux FSIN ont affirmé leur capacité de répondre aux exigences du GC en matière de stockage et de traitement des données classées Protégé B. Cette affirmation sera mise à l'épreuve par le GC au fur et à mesure qu'il obtiendra des services d'informatique en nuage pour les scénarios utilisant des données classées Protégé B. Pour cette raison, le GC a déclaré que seulement les données classées jusqu'à Protégé B peuvent être déployées dans un nuage public.

Chiffrement des données

Lorsque l'on utilise des services d'informatique en nuage, le chiffrement peut offrir un degré élevé de séparation afin de protéger les renseignements personnels et d'autres renseignements de nature délicate. Les données chiffrées au moyen d'un algorithme cryptographique rigide sont protégées contre toute personne qui n'a pas la clé de déchiffrement. Le GC exigera que :

- toutes les données protégées en transit et non utilisées qui sont hébergées dans le nuage soient chiffrées de manière appropriée;
- le GC conserve le contrôle exclusif des clés de chiffrement.

Il convient de mentionner que si les données chiffrées doivent être traitées dans le nuage au moyen d'une application, elles devront être déchiffrées au préalable. Par conséquent, une photo non chiffrée des données sensibles serait stockée temporairement dans le nuage avant d'être écrasée. Le GC continuera d'examiner les techniques disponibles afin d'atténuer ce risque et d'empêcher la divulgation de données à des personnes non autorisées. Parmi les techniques d'atténuation possibles, on compte l'anonymisation des données et l'isolement du matériel.

Clauses contractuelles types pour le nuage

Les autorités contractantes doivent veiller à ce que tous les contrats conclus avec un FSIN comprennent des clauses qui l'obligent de divulguer tous les incidents d'accès non autorisé aux données, y compris ceux qui sont permis en vertu d'une ordonnance du tribunal, le cas échéant, et à moins que la loi l'interdise au FSIN. Dans certains cas, comme celui d'une ordonnance de la Cour de surveillance du renseignement étranger des États-Unis (FISC), une

telle divulgation est interdite en vertu de la loi américaine. Le GC peut demander aux FSIN de lui fournir leurs procédures pour gérer le conflit entre leurs obligations contractuelles et les lois applicables.

Équilibrer les risques en matière de sécurité et les avantages commerciaux

Titres de la section

- Vieillissement de l'infrastructure de la TI
- Lacunes en matière de pratiques de base concernant la cybersécurité
- Disponibilité de solutions hors-nuage
- Plans du GC visant une transformation numérique

Jusqu'ici, le présent document met l'accent sur les risques les plus complexes liés à l'adoption du nuage public. À cette étape, on se demande peut-être que si le GC a considéré tous les risques, pourquoi adopte-il le nuage public? La réponse simple à cette question est qu'il existe d'importants avantages commerciaux liés à l'utilisation des services d'informatique en nuage. Lorsque l'on évalue les risques liés au nuage, il faut aussi tenir compte des risques ayant trait au statu quo, et tenir compte des moyens par l'entremise desquels le nuage pourrait aider le GC à gérer ces risques, notamment :

- vieillissement de l'infrastructure de la TI;
- lacunes en matière de pratiques de base concernant la cybersécurité;
- disponibilité de solutions hors-nuage;
- plans du GC visant une transformation numérique.

Vieillissement de l'infrastructure de la TI

Vieillissante et essentielle à la mission du GC, l'infrastructure de la TI risque de tomber en panne et doit être renouvelée. La transformation de l'infrastructure de la TI se fait plus lentement que prévu, en partie en raison de la complexité et des défis de la consolidation des centres de données, des réseaux et des systèmes de courriel de 43 ministères. Comme il est indiqué dans l'Examen de l'harmonisation des ressources de Services partagés Canada, l'informatique en nuage présente une importante occasion de relever ces défis et de réaliser des économies. Un facteur clé de l'adoption de l'informatique en nuage est la nécessité d'éliminer graduellement la fonction de gestion des actifs vieillissants et d'accroître l'utilisation des services d'informatique en nuage offerts sur le marché, optimisant les ressources.

Lacunes en matière de pratiques de base concernant la cybersécurité

Le nombre croissant d'incidents de sécurité a démontré l'inégalité de la sécurité des systèmes informatiques du GC. Les leçons retenues ont mis en évidence les défis liés à la capacité du GC de repérer rapidement les actifs et d'appliquer en temps opportun des mesures correctives au regard des vulnérabilités connues, de sorte que le GC est exposé à des cybermenaces. Le passage à l'informatique en nuage offre au GC la possibilité de :

- déployer rapidement un environnement virtuel sécurisé;
- adapter son approche au regard de la gestion des actifs et aborder les questions de sécurité dès le départ.

Les FSIN disposent d'un budget important pour entretenir, corriger et sécuriser leur infrastructure d'informatique en nuage. Cela signifie que les FSIN peuvent :

- atténuer de nombreux risques communs que rencontrent les organisations gouvernementales;
- offrir une sécurité globale beaucoup plus solide.

En outre, les FSIN de premier rang soumettent leurs services et leurs procédures à de nombreux audits menés par des tierces parties, et ils se conforment à de nombreuses normes de certification de la sécurité reconnues à l'échelle internationale comme ISO 27001 afin de fournir des garanties à leurs clients.

Disponibilité de solutions hors-nuage

De plus en plus dans le secteur industriel, on offre seulement des solutions d'informatique en nuage public ou on concentre ses efforts sur les services d'informatique en nuage. L'expression « né dans le nuage » signifie qu'une solution particulière a été conçue pour résider dans un nuage public à l'échelle nationale et qu'il n'existe aucun autre logiciel équivalent. Si l'on exclut les solutions d'informatique en nuage de la TI du GC, on limite le nombre de solutions disponibles.

Plans du GC visant une transformation numérique

La demande en compétences et en capacités de la TI du GC dépasse l'offre disponible. Le GC entend suivre la tendance mondiale visant à améliorer les services numériques pour les citoyens, ce qui est tout à fait possible au moyen des services d'informatique en nuage. De nombreux gouvernements ont mis en œuvre des politiques « d'informatique en nuage d'abord », y compris les autres pays du Groupe des cinq, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande. Le Canada est le seul pays du Groupe des cinq à ne pas

avoir de politique d'informatique en nuage d'abord. Le manquement à intégrer le nuage au paysage numérique du GC aura une incidence sur sa capacité de réaliser en temps opportun la vision numérique pour le GC.

Sommaire

Les récentes mises à jour apportées à la Politique sur la gestion de la technologie de l'information reflètent la stratégie de l'informatique en nuage d'abord du GC. Les ministères doivent donc considérer l'utilisation des services d'informatique en nuage comme principale option de prestation pour le stockage des données en tenant compte des besoins opérationnels. Au moment d'envisager l'utilisation des services d'informatique en nuage, les ministères doivent garder à l'esprit ce qui suit :

- À l'heure actuelle, seulement les données allant jusqu'au niveau Protégé B inclusivement doivent être stockées dans un environnement en nuage public commercial.
- S'il répond à leurs besoins, les ministères pourront utiliser le contrat sur l'informatique en nuage protégée (qui est en cours d'établissement) pour accéder aux services d'informatique en nuage.
- Les ministères qui choisissent de se procurer eux-mêmes des services d'informatique en nuage devraient :
    - évaluer les risques inhérents pour la souveraineté des données, la résidence des données et la sécurité des données;
    - appliquer des mesures d'atténuation pertinentes.
- L'utilisation des services d'informatique en nuage est assujettie aux directives suivantes :
    - Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS);
    - Orientation relative à la résidence des données électroniques.

Prochaines étapes

▾ Titres de la section

- Élaborer des lignes directrices sur le chiffrement des données pour le nuage
- Établir des clauses contractuelles types pour le nuage
- Lancement de l'approvisionnement en informatique en nuage protégé

Le GC est responsable de :

- protéger la confidentialité, l'intégrité et la disponibilité de l'information et des actifs de la TI du GC;
- mettre en œuvre les mesures appropriées pour assurer la protection des données.

Cette responsabilité demeure la même, qu'elle soit assumée sur place, dans une installation du GC, ou hors site, dans un environnement en nuage. L'informatique en nuage n'y change rien, mais sa portée mondiale et son infrastructure partagée entraînent de nouveaux défis. Une approche équilibrée est nécessaire pour :

- adopter l'informatique en nuage comme modèle de prestation de services de rechange pour la prestation des services de la TI;
- gérer les risques pour la souveraineté des données.

Le Conseil d'examen de l'architecture intégrée (CEAI) du GC :

- établit l'orientation de la TI organisationnelle pour l'ensemble du gouvernement;
- joue un rôle clé dans la gestion des risques liés à l'adoption de l'informatique en nuage.

Le CEAI se compose de représentants d'organisations de partout au sein du GC, notamment :

- responsables opérationnels tels que l'Agence du revenu du Canada (ARC) et Emploi et Développement social Canada (EDSC);
- fournisseurs de services tels que Services partagés Canada (SPC) et Services publics et Approvisionnement Canada (SPAC);
- principaux organismes de sécurité tels que le Centre de la sécurité des télécommunications Canada (CSTC) et le Secrétariat du Conseil du Trésor du Canada (SCT).

Le Conseil entreprendra l'examen de toutes les demandes de services d'informatique en nuage en empruntant une perspective d'architecture et une perspective de risque afin d'atténuer le plus possible les risques soulevés dans ce document.

Dans le but de réaliser tous les avantages de l'informatique en nuage, tout en limitant l'exposition au risque du GC, les prochaines étapes suivantes doivent être franchies :

Élaborer des lignes directrices sur le chiffrement des données pour le nuage

Dans le présent document, on explique comment le GC assurera le contrôle des clés de chiffrement des données hébergées dans un environnement en nuage afin d'atténuer les préoccupations d'accès non autorisé (hiver 2017-2018).

Établir des clauses contractuelles types pour le nuage

Ces clauses obligeront le FSIN à divulguer au GC tout accès non autorisé aux données (y compris celles qui ont été obtenues en vertu d'une ordonnance du tribunal), à moins que le FSIN ne soit interdit par la loi de le faire (exercice financier 2018-2019).

Lancement de l'approvisionnement en informatique en nuage protégé

SPC et SPAC seront en mesure d'utiliser l'Orientation relative à la résidence des données électroniques, l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) et le Profil de contrôle de sécurité pour les services de la TI du GC fondés sur l'informatique en nuage pour lancer l'approvisionnement en informatique en nuage protégé en 2018.

Les ministères et organismes utiliseront également l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) pour sécuriser les services qu'ils déploient dans le nuage.

Annexe A : Réponses du gouvernement concernant la souveraineté des données

Lorsqu'il s'agit d'examiner la question de souveraineté des données, il est important de déterminer quelles mesures d'atténuation les autres gouvernements ont mises en œuvre. Le tableau suivant donne un aperçu global :

Mesure d'atténuation	Avantages	Inconvénients	Qui fait quoi?
Résidence des données Exige que certaines données soient stockées dans les limites géographiques du pays.	La résidence des données permet de maintenir : • accès aux données du GC; • confiance du public.	• La résidence des données n'atténue pas le risque d'application de lois étrangères.	Colombie-Britannique : Les données doivent être stockées au Canada. La France et l'Allemagne ont aussi des exigences en matière de résidence des données.

Mesure d'atténuation	Avantages	Inconvénients	Qui fait quoi?
Chiffrement des données Rend les données du Canada opaques pour le fournisseur de services d'informatique en nuage (FSIN).	• Rend les données du Canada opaques pour le FSIN.	Chiffrement • peut entraîner une réduction de la fonctionnalité; • tient le GC responsable de gérer les clés de chiffrement.	Le R.-U. a publié des conseils sur le chiffrement des données.
Masquage des données Protège les données de nature délicate en les stockant à un emplacement physique du GC; les données stockées dans le nuage sont semblables sur le plan structurel, mais elles ne sont pas réelles.	• Rend anonymes les données de nature délicate du Canada.	Le masquage : • peut entraîner une réduction de la fonctionnalité; • tient le GC responsable de gérer l'infrastructure de masquage des données du GC.	Inconnu

Mesure d'atténuation	Avantages	Inconvénients	Qui fait quoi?
Veiller à ce que les FSIN obtiennent les accréditations de sécurité exigées Veiller à ce que les FSIN obtiennent les certificats de sécurité reconnus à l'échelle internationale comme ISO 27001 [1] .	• Les FSIN se conforment aux mesures de contrôle de la sécurité et aux mesures de protection des renseignements personnels du GC.	• Les certificats de sécurité n'ont pas pour effet d'atténuer les lois étrangères.	Canada : Les mesures de contrôle ITSG-33 [2] du CSTC ont été mises en correspondance avec ISO 27001 et SOC 2 [3]. R.U. : IS027001 est approprié pour les données classées comme officielles.
Utiliser des clauses contractuelles types avec les FSIN Inclut les clauses qui obligent le FSIN à maintenir la confidentialité.	• Le Canada dispose de mécanismes pour faire respecter les lois canadiennes et conserver la propriété des données.	• Il n'est pas évident comment un FSIN serait en mesure de gérer un conflit entre les obligations contractuelles et les lois étrangères.	Canada : Le FSIN doit se conformer à la Loi sur la protection des renseignements personnels. L'Union européenne a commencé à émettre des clauses contractuelles modèles visant la protection des données personnelles.

Mesure d'atténuation	Avantages	Inconvénients	Qui fait quoi?
Confier les données à une entreprise canadienne Permet de veiller à ce que le FSIN utilise une entreprise canadienne pour contrôler l'accès au nuage.	• L'accès des FSIN est contrôlé par une entreprise canadienne.	• Seulement un FSIN dans un pays a adopté ce modèle. • Le GC ne sait pas que cette mesure d'atténuation a été mise à l'essai dans les tribunaux.	Allemagne : Microsoft a créé un nuage souverain dont l'accès est contrôlé par une firme de télécommunications allemande.
Rationalisation des catégories de données Harmonise les catégories de données avec les capacités de sécurité commerciale.	• Les catégories de données ont été modernisées pour l'environnement cybernétique actuel. • Le Canada peut déterminer où les mesures de contrôle commerciales sont adéquates.	• La rationalisation des catégories de données n'a pas pour effet d'atténuer les lois étrangères.	Le R.-U. a rationalisé six catégories en trois catégories. Le R.-U. a aussi décidé que les données classées comme officielles peuvent être sécurisées au moyen de mesures de contrôle commerciales.

Mesure d'atténuation	Avantages	Inconvénients	Qui fait quoi?
Limitation des catégories de données stockées dans le nuage Les données d'intérêt non national sont appropriées pour le nuage public.	• Le Canada sait quel niveau de données est approprié pour le nuage public.	• Sans objet	Canada : Le nuage peut être utilisé pour les données allant jusqu'au niveau Protégé B inclusivement. R.-U. : Le nuage peut être utilisé pour les données classées comme officielles.

1 L'acronyme ISO correspond à « International Organization for Standardization », désignant l'Organisation internationale de normalisation (ISO).

2 L'acronyme ITSG correspond à « Information Technology Security Guidance », désignant les Conseils en matière de sécurité de la technologie de l'information (ITSG).

3 L'acronyme SOC correspond à « System and Organization Controls », désignant les mesures de contrôle pour les systèmes et l'organisation.

Notes en bas de page

1 Les ministères clés sont Services partagés Canada, Services publics et Approvisionnement Canada ainsi que le Centre de la sécurité des télécommunications Canada.

2 Au Canada, la « souveraineté des données » désigne le droit du Canada de contrôler l'accès aux données numériques ainsi que la divulgation des données numériques qui sont assujetties aux lois canadiennes seulement.

3 La « résidence des données » désigne l'emplacement physique ou géographique des données numériques d'une organisation.

4 L'acronyme ITSG correspond à « Information Technology Security Guidance », et il désigne les Conseils en matière de sécurité de la TI.

© Sa Majesté la Reine du chef du Canada, représentée par le président du Conseil du Trésor, 2018,
ISBN : 978-0-660-27234-4

Date de modification :
2018-07-13